Remarks

Claims 1-19 are pending.

Response to Examiner's Response to Arguments

On page 2 of the present Office Action, the Examiner provides a two-paragraph "Response to Arguments". That response is respectfully traversed.

In the present Office Action, the Examiner rejects Claims 1-19 on the ground of being "unpatentable as in the previous Office Action". The Examiner concludes in the Response to Arguments[1], that "the crux of [Applicants'] argument is that 'encoding' and 'decoding' are not obvious in view of the prior art." It is respectfully submitted that the Examiner's sole focus on those two terms (*i.e.*, the word "encoding" and the word "decoding"), without proper consideration of Applicants' claimed invention, taken as a whole, demonstrates that the Examiner has, in fact, not considered the rest of the refined arguments as set forth on pages 4 and 5 of the previous Response with respect to Claim 1.[2] There it is stated:

---

[1] Applicants' attorney agrees that the Remarks of the previous Response are found on pages 2-7 thereof, and that pages 2 and 3 of that Response discuss the cited references and set forth the substance of Claim 1. Next, in the Examiner's Response, the Examiner concludes that: "Page 4 gives 'encoding' and 'decoding' as a novel feature. The rest of page 4 and part of page 5 summarize the references as well." Actually, what is said on page 4 of the previous Response is that "nothing in Van Meter et al. teaches or suggests 'encoding' and 'decoding' as set forth in the refined recital of Claim 1" and that "Myers et al., which merely discloses that it is advantageous to encrypt communication between trusted nodes of a communication network, adds nothing to Van Meter et al. regarding any enable code for a block of a controller, obtaining an identification and an identifier from such enable code, and enabling a block of a controller when such obtained identification is equal to a unique identification of such controller and when such obtained identifier is equal to an identifier of such block." It was also stated, as is discussed on pages 3 and 11 of the present Response, that Van Meter et al. does not teach or suggest that recital. Applicants' attorney has never argued that the word "encoding" or the word "decoding" is novel. Hence, it is respectfully submitted that the Examiner's conclusion about the word 'encoding' and the word 'decoding' as being a novel feature is incorrect. In view of the above, the Examiner's conclusion that the "rest of page 4 and part of page 5" of the previous Response merely "summarize the references as well" is also incorrect. The next two sentences of the first paragraph of the Examiner's Response to Arguments solely pertain to dependent Claims 2-19, which are dealt with later in the present Response. In view of the forgoing, it is respectfully submitted that it is clear that the Examiner has incorrectly concluded that "[t]hus, the crux of [Applicants'] argument is that 'encoding' and 'decoding' are not obvious in view of the prior art."

[2]

> A determination under 35 U.S.C. 103 should rest on all the evidence and should not be influenced by any earlier conclusion. *See, e.g., Piasecki*, 745 F.2d at 1472-73, 223 USPQ at 788; *In re Eli Lilly & Co.*, 902 F.2d 943, 945, 14 USPQ2d 1741, 1743 (Fed. Cir. 1990). Thus, once the applicant has presented rebuttal evidence, Office personnel should reconsider any initial obviousness determination in view of the entire record. *See, e.g., Piasecki*, 745 F.2d at 1472, 223 USPQ at 788; *Eli Lilly*, 902 F.2d at 945, 14 USPQ2d at 1743. All the proposed rejections and their bases should be reviewed to confirm their correctness. Only then should any rejection be imposed in an Office action. The Office action should clearly communicate the Office's findings and conclusions, articulating how the conclusions are supported by the findings. Where applicable, the findings should clearly articulate which portions of the reference support any rejection.
>
> MPEP § 2144.08.

> It is further submitted that nothing in Van Meter et al. teaches or suggests encoding an enable code for a block of a controller, decoding such enable code to obtain a decoded identification and a decoded identifier, and enabling such block of such controller when such decoded identification is equal to a unique identification of such controller and such decoded identifier is equal to an identifier of such block. Myers et al., which merely discloses that it is advantageous to encrypt communication between trusted nodes of a communication network, adds nothing to Van Meter et al. regarding any enable code for a block of a controller, obtaining an identification and an identifier from such enable code, and enabling a block of a controller when such obtained identification is equal to a unique identification of such controller and when such obtained identifier is equal to an identifier of such block.

The initial burden[3] is on the Examiner to provide some reasonable suggestion of the desirability of doing what the inventors have done and claimed.

> To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references.

Ex parte Clapp, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985).

In the previous Office Action, as to the refined recitals of: (1) encoding an enable code for a block of a controller; (2) decoding such enable code to obtain a decoded identification and a decoded identifier; and (3) enabling such block of such controller when such decoded identification is equal to a unique identification of such controller and such decoded identifier is equal to an identifier of such block, the Examiner refers, in all three instances, to page 72 of "VISA: Netstation's Virtual Internet SCSI Adapter" (Van Meter et

---

3

> The legal concept of prima facie obviousness is a procedural tool of examination which applies broadly to all arts. It allocates who has the burden of going forward with production of evidence in each step of the examination process. *See In re Rinehart*, 531 F.2d 1048, 189 USPQ 143 (CCPA 1976); *In re Linter*, 458 F.2d 1013, 173 USPQ 560 (CCPA 1972); *In re Saunders*, 444 F.2d 599, 170 USPQ 213 (CCPA 1971); *In re Tiffin*, 443 F.2d 394, 170 USPQ 88 (CCPA 1971), *amended*, 448 F.2d 791, 171 USPQ 294 (CCPA 1971); *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967), *cert. denied*, 389 U.S. 1057 (1968). The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness.

MPEP § 2142.

al.). There the Examiner states "derived virtual device in which the set of types of access is set as policy by owner, also Figure 1".

A detailed discussion of Van Meter et al. is set forth on page 3 of the previous response. The Examiner provides no substantive comment to that discussion. Also, the Examiner's finding does not clearly articulate which specific portions of that reference support the above three elements of Claim 1. It is respectfully submitted that it is totally unclear how the Examiner might apply the above single quote or page 72 of Van Meter et al. to one, much less all three of the above recitals. No attempt to clarify this point is set forth in the present Office Action.

Furthermore, the Examiner provides no response to Applicants' argument that Myers et al., which merely discloses that it is advantageous to encrypt communication between trusted nodes of a communication network, adds nothing to Van Meter et al. regarding any enable code for a block of a controller, obtaining an identification and an identifier from such enable code, and enabling a block of a controller when such obtained identification is equal to a unique identification of such controller and when such obtained identifier is equal to an identifier of such block.

In the previous Office Action, the Examiner stated that Van Meter et al. does not teach "functional" in the context of the claims. The Examiner also stated that Myers et al. teaches "such 'functional' nature (page 131, the customer requests which are requests for functions such as transactions) for the motivation of decentralizing information control". Even if Myers et al. might suggest the single word "functional," although that is not admitted within the context of Claim 1, the Examiner has not presented any convincing argument as to how that one word might be combined with the teachings of Van Meter et al. to teach or suggest a functional block having an identifier for a controller having a unique identification, an enable code for a functional block of a controller, or enabling a functional block of a controller.

Furthermore, the only "motivation" that the Examiner presents in either of the two Office Actions to combine the references is the mere conclusion[4] "the motivation of decentralizing information control". Actually, this conclusion is a mischaracterization of Myers et al. (page 131) (***emphasis added***), which deals with a "model for controlling information ***flow*** in systems with mutual distrust and decentralized authority". As was discussed on page 2 of the previous Response, that model allows users to share information

[4] Conclusory statements of similarity or motivation, without any articulated rationale or evidentiary support, do not constitute sufficient factual findings. MPEP § 2144.08.

with distrusted code (*e.g.*, downloaded applets), yet still control how that code disseminates the shared information to others. The model purports to improve on existing multilevel security models by allowing users to declassify information in a decentralized way, by improving support for fine-grained data sharing, and by allowing users to control the flow of their information without imposing the rigid constraints of a traditional multilevel security system. At heading 3 of Myers et al., it discusses "Decentralized Information Flow Control," which is far removed from the refined recital of a controller having a unique identification, an enable code for a functional block of a controller, or enabling a functional block of a controller of Claim 1.

In view of the above, it is respectfully submitted that the Examiner has not presented a convincing line of reasoning as to why the ordinary artisan would have found Claim 1 to have been obvious in light of the teachings of the references.

Pages 5-7 of the previous Response dealt with the patentability of dependent Claims 2-19. It is respectfully submitted that the Examiner's sole focus on the two terms 'encoding' and 'decoding' also demonstrates that the Examiner has, in fact, ignored the specific arguments directed to Claims 2, 3, 5, 15 and 19. The recitals of those claims further patentably distinguish over the references. In other words, those recitals are not "typical of the aspects of claim 1 that were discussed in pages 2-5" of the previous Response as was incorrectly stated by the Examiner in the present Response to Arguments.

As to Claims 2, 3 and 5, the previous Response (page 5) made clear that those claims do not recite "typical purchasing/selling situations" as was the conclusion of the Examiner.[5]

Moreover, to the extent that the Examiner might take the position that the refined recitals of Claim 2 (selling an enable code for a functional block of a controller based upon a unique identification of such controller and an identifier of such functional block), Claim 3 (purchasing an enable code for a functional block of a controller based upon a unique identification of such controller and an identifier of such functional block) and Claim 5 (entering an identifier of a functional block and a unique identification of a controller into an encoder; encoding a purchase code as an enable code from such identifier of such functional block and such unique identification of such controller; and selling such purchase code) were

[5] It would seem that under that conclusion, any claim of any patent application of any inventor directed to any purchasing or selling methodology, no matter how artfully refined, would be *per se* unpatentable. It is respectfully submitted that such a position cannot plausibly be maintained.

well known, then the Examiner was (in the previous Response) and is, again, in this Response respectfully requested to cite a reference within the context of Applicants' claims.

> It would not be appropriate for the examiner to take official notice of facts without citing a prior art reference where the facts asserted to be well known are not capable of instant and unquestionable demonstration as being well-known. For example, assertions of technical facts in the areas of esoteric technology or specific knowledge of the prior art must always be supported by citation to some reference work recognized as standard in the pertinent art.

In re Ahlert, 424 F.2d 1088, 1091, 165 USPQ 418, 420-21 (CCPA 1970).

Furthermore, the Examiner's reliance on the "example of a banking e-commerce" of Myers et al. (page 131) is misplaced. Myers et al. teaches bank software and bank transactions, such as withdrawing and depositing money, but there is no teaching or suggestion about purchasing or selling the recited "enable code" of Claims 1-3, or about selling such a purchase code that was encoded as an enable code of Claim 5.

There is nothing "typical" about the refined recitals of Claims 2, 3 and 5. Instead, it appears that the Examiner improperly focuses upon the single word "purchasing" or the single word "selling" instead of the claimed invention, taken as a whole. Hence, it is submitted that Applicants' attorney has adequately traversed the Examiner's conclusions that dependent Claims 2, 3 and 5 recite "typical purchasing/selling situations" or are well-known.[6]

Based upon the above, it is respectfully submitted that the Examiner has not met the requisite burden of proof and has failed to cite a prior art reference as applied to the refined recital of Claims 2, 3 and 5, taken as a whole, since the "facts" asserted to be well known are clearly not capable of instant and unquestionable demonstration as being well-known.

> If applicant adequately traverses the examiner's assertion of official notice, the examiner must provide documentary evidence in the next Office action if the rejection is to be maintained. *See* 37 CFR 1.104(c)(2). *See also Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697 ("[T]he Board [or examiner] must point to some concrete evidence in

---

[6] Applicants' attorney has not argued that the word "purchasing" or the word "selling" is novel. Instead, it is submitted that what is purchased and what is sold within the context of Claim 1 and Claims 2, 3 or 5 is novel and non-obvious and, thus, is not well-known.

> To adequately traverse such a finding, an applicant must specifically point out the supposed errors in the examiner's action, which would include stating why the noticed fact is not considered to be common knowledge or well-known in the art. *See* 37 CFR 1.111(b). *See also Chevenard*, 139 F.2d at 713, 60 USPQ at 241.

MPEP § 2144.04 C.

> the record in support of these findings" to satisfy the substantial evidence test).

MPEP § 2144.03, C.

Hence, it is respectfully submitted that the rejection of Claims 2, 3 and 5 cannot properly be maintained in the present Office Action, since the Examiner has provided no documentary evidence directed to the refined recitals of those claims in either of the two Office Actions.

It is respectfully submitted that the Examiner makes the same error with regard to Claim 15 (employing a block number as an identifier of a functional block; employing a unique controller number as a unique identification of a controller; inputting such block number and such unique controller number into an encryption algorithm; outputting a purchase code as an enable code from such encryption algorithm; inputting such purchase code into a decryption algorithm; outputting a decrypted block number and a decrypted controller number from such decryption algorithm; and enabling a functional block of such controller when such decrypted block number is equal to such identifier of such functional block and such decrypted controller number is equal to such unique identification) and Claim 19 (displaying a unique controller number and a block number; informing a supplier of such unique controller number and such block number; and inputting such unique controller number and such block number into an encryption algorithm at a facility of such supplier), since the previous Response (pages 6 and 7) made clear that the refined recital of Claims 15 and 19 do not recite "typical purchasing/selling situations" as was incorrectly stated by the Examiner.

Again with regard to the Examiner's sole focus on the two terms 'encoding' and 'decoding', a detailed description of the specific respective concepts of 'encrypting' and 'decrypting' is set forth in the Background Information on pages 2 and 3 of the present specification. Applicants' attorney has never argued that any of those four individual words is novel. Moreover, the Examiner's focus is taken as evidence that the Examiner has expressly ignored Applicants' invention taken as a whole.[7]

7

> To reach a proper determination under 35 U.S.C. 103, the examiner must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of applicant's disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the "differences," conduct the search and evaluate the "subject matter as a whole" of the invention. The tendency to resort to "hindsight" based upon applicant's disclosure is often

> [W]hen evaluating the scope of a claim, ***every*** limitation in the claim must be considered. Office personnel may ***not*** dissect a claimed invention into discrete elements and then evaluate the elements in isolation. Instead, ***the claim as a whole must be considered***. *See, e.g., Diamond v. Diehr*, 450 U.S. at 188-89, 209 USPQ at 9.

MPEP § 2106 (***emphasis added***).

In view of the above, it is respectfully submitted that the Examiner errs when stating that "[u]nless Applicant[s are] willing to state ... that 'encoding' and 'decoding' are not well known in the relevant art ..., Applicant[s'] arguments are not persuasive." Hence, it is respectfully submitted that the Examiner has not properly considered Applicants' invention, taken as a whole, has ignored the refined arguments as set forth on pages 4 and 5 of the previous Response with respect to Claim 1, has ignored the refined arguments as set forth on pages 5-7 of the previous Response with respect to Claims 2, 3, 5, 15 and 19, and has not provided documentary evidence or a convincing line of reasoning directed to the refined recitals of those claims in either of the two Office Actions.

Rejections Under 35 U.S.C. § 103(a)

The Examiner rejects Claims 1-19 on the ground of being unpatentable over "A Decentralized Model for Information Flow Control" (Myers et al.) and "VISA: Netstation's Virtual Internet SCSI Adapter" (Van Meter et al.).

Myers et al. discloses a model for controlling information flow in systems with mutual distrust and decentralized authority. The model allows users to share information with distrusted code (*e.g.*, downloaded applets), yet still control how that code disseminates the shared information to others. The model purports to improve on existing multilevel security models by allowing users to declassify information in a decentralized way, by improving support for fine-grained data sharing, and by allowing users to control the flow of their information without imposing the rigid constraints of a traditional multilevel security system.

Myers et al. discloses that when a computational environment contains many trusted nodes connected by a network, the communication links between the nodes must be trusted, which can be accomplished by encrypting communication between nodes. Myers et al. also discloses that information flow control is vital for large or extensible systems. In a

---

> difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

MPEP § 2142.

small system, preventing improper propagation of information is easy: you don't pass data to code whose implementation is not completely trusted. This simple rule breaks down in larger systems, because the trust requirement is transitive: any code the data might travel to must also be trusted, requiring complete understanding of the code. As the system grows larger and more complex, and incorporates distrusted code (*e.g.*, web applications), complete trust becomes unattainable.

As shown in Figure 2 of Myers et al., a bank serves many customers, each of whom would like to keep his data safe from other customers and non-customers. In addition, the bank stores private information, such as its current assets and investments, that it would like to keep safe from all customers and non-customers. In this banking example, the bank receives periodic requests from each customer, for example, to withdraw or deposit money. Each request should be able to observe only information that is owned by that customer, and none of the bank's private data. The bank is better than real banks in that it allows customers to control dissemination of their account information; each customer has a distinct information flow policy for his account information, which prevents the bank from leaking the information to another party.

Van Meter et al. discloses a Virtual Internet SCSI Adapter (VISA) to evaluate the performance impact on a host operating system of using IP to communicate with peripherals, especially storage devices. Connecting peripherals directly to a network allows sharing of resources and improves system configuration flexibility. Network clients can access peripherals, such as network-attached storage devices (NASDs), without the intervention of a server.

A Netstation project concentrates on operating systems, network protocols, hardware mechanisms, and security and sharing models for network-attached peripherals. Some of the goals of the project are to demonstrate: (1) that IP can provide acceptable performance in a host operating system when used to access peripherals, (2) that IP can be implemented efficiently inside network-attached peripherals, and (3) that a derived virtual device model enables efficient, secure use of network-attached peripherals (NAPS).

Netstation is a heterogeneous distributed system composed of processor nodes (CPU/Memory) and network-attached peripherals. The peripherals are attached to a shared Local Area Network as shown in Figure 1 of Van Meter et al. The peripherals include displays, magnetic disks, a RAM disk, a camera and a keyboard/mouse. Because the peripherals are attached to an open network with both trusted and untrusted nodes on the net, security at NAPS is critical. A model, referred to as a derived virtual device (DVD), provides

a protected execution context at the device, allowing direct use of the devices by untrusted clients, such as user applications. The owner of a device defines the security policy, downloads a description to the NAP, and the NAP enforces the policy. This allows the owner to define a set of resources and operations allowed. Thus, a camera can be granted write access to only a specific region of a frame buffer, or a user application can be given read-only access to a DVD which represents a disk-based file or disk partition.

Claim 1 recites, *inter alia*, a method of enabling at least one functional block having an identifier for a controller having a unique identification. The method comprises encoding an enable code for the functional block of the controller based upon the unique identification of the controller and the identifier of the functional block; decoding the enable code for the functional block of the controller to obtain a decoded identification and a decoded identifier; and enabling the functional block of the controller when the decoded identification is equal to the unique identification and the decoded identifier is equal to the identifier of the functional block.

The Examiner states that Van Meter et al. does not teach "functional" in the context of the claims.

The Examiner further states that Myers et al. teaches "such 'functional' nature (page 131, the customer requests which are requests for functions such as transactions) for the motivation of decentralizing information control". The Examiner also states that each of: (1) "encoding an enable code for the [] block of said controller based upon the unique identification of said controller and the identifier of said [] block"; (2) "decoding the enable code for the [] block of said controller to obtain a decoded identification and a decoded identifier"; and (3) "enabling the [] block of said controller when said decoded identification is equal to said unique identification and said decoded identifier is equal to the identifier of said [] block" are taught by Van Meter et al. (page 72, "derived virtual device in which the set of types of access is set as policy by owner, also Figure 1"). These statements are respectfully traversed as applied to the refined recital of Applicants' claims.

As employed in the application, the term "encoding" means "encrypting, enciphering, or converting a set of intelligible information into a corresponding cipher coded set of information." Also, the term "decoding" means "decrypting, deciphering, or converting a cipher coded set of information into a corresponding set of intelligible information." *See* page 5, line 29 through page 6, line 3 of the specification.

It is submitted that nothing in Van Meter et al. teaches or suggests "encoding" or "decoding" as set forth in the refined recital of Claim 1. Van Meter et al., which teaches

that a peripheral device, such as a camera, can be granted write access to only a specific region of a frame buffer or that a user application can be given read-only access to a disk-based file or disk partition, does not teach or suggest encrypting, enciphering, or converting a set of intelligible information into a corresponding cipher coded set of information, or decrypting, deciphering, or converting a cipher coded set of information into a corresponding set of intelligible information.

It is further submitted that nothing in Van Meter et al. teaches or suggests encoding an enable code for a block of a controller, decoding such enable code to obtain a decoded identification and a decoded identifier, and enabling such block of such controller when such decoded identification is equal to a unique identification of such controller and such decoded identifier is equal to an identifier of such block. Myers et al., which merely discloses that it is advantageous to encrypt communication between trusted nodes of a communication network, adds nothing to Van Meter et al. regarding any enable code for a block of a controller, obtaining an identification and an identifier from such enable code, and enabling a block of a controller when such obtained identification is equal to a unique identification of such controller and when such obtained identifier is equal to an identifier of such block.

In the previous Office Action, the Examiner stated that Van Meter et al. does not teach "functional" in the context of the claims. The Examiner also stated that Myers et al. teaches "such 'functional' nature (page 131, the customer requests which are requests for functions such as transactions) for the motivation of decentralizing information control". Even if Myers et al. might suggest the single word "functional," although that is not admitted within the context of Claim 1, the Examiner has not presented any convincing argument as to how that one word might be combined with the teachings of Van Meter et al. to teach or suggest a functional block having an identifier for a controller having a unique identification, an enable code for a functional block of a controller, or enabling a functional block of a controller.

Furthermore, the only "motivation" that the Examiner presents in either of the two Office Actions to combine the references is the mere conclusion "the motivation of decentralizing information control". Actually, this conclusion is a mischaracterization of Myers et al. (page 131) (***emphasis added***), which deals with a "model for controlling information ***flow*** in systems with mutual distrust and decentralized authority". As was discussed on page 2 of the previous Response, that model allows users to share information with distrusted code (*e.g.*, downloaded applets), yet still control how that code disseminates

the shared information to others. The model purports to improve on existing multilevel security models by allowing users to declassify information in a decentralized way, by improving support for fine-grained data sharing, and by allowing users to control the flow of their information without imposing the rigid constraints of a traditional multilevel security system. At heading 3 of Myers et al., it discusses "Decentralized Information Flow Control," which is far removed from the refined recital of a controller having a unique identification, an enable code for a functional block of a controller, or enabling a functional block of a controller of Claim 1.

In view of the above, it is respectfully submitted that the Examiner has not presented a convincing line of reasoning as to why the ordinary artisan would have found Claim 1 to have been obvious in light of the teachings of the references.

The references, whether taken alone or in combination, do not teach or suggest the refined recital of Claim 1.

Accordingly, for the above reasons, Claim 1 patentably distinguishes over the references.

Claims 2-19 depend directly or indirectly from Claim 1 and patentably distinguish over the references for the same reasons.

The Examiner states that Claims 2, 3 and 5 recite limitations regarding "typical purchasing/selling situations". The Examiner states that purchasing and selling are well known in the art of e-commerce for the motivation of permitting transactions, and that Myers et al. (page 131) teaches banking e-commerce. These statements are traversed as applied to the refined recital of Applicants' claims, which do not recite "typical purchasing/selling situations". To the extent that the Examiner takes the position that the recitals of Claims 2, 3 and 5 are well known, then it is respectfully requested that the Examiner cite a reference within the context of Applicants' claims.

Since the references do not teach or suggest encoding or decoding an enable code, they clearly do not contemplate or suggest selling such enable code for a functional block of a controller based upon a unique identification of such controller and an identifier of such functional block as set forth in Claim 2, or purchasing such enable code for a functional block of a controller based upon a unique identification of such controller and an identifier of such functional block as set forth in Claim 3. Although Myers et al. teaches bank software and bank transactions, such as withdrawing and depositing money, there is no teaching or suggestion about purchasing or selling the recited "enable code" of Claims 1-3. Van Meter et al., which discloses peripherals on a local area network, adds nothing to Myers et al. in this

regard. Therefore, it is submitted that Claims 2 and 3 further patentably distinguish over the references.

Furthermore, Claim 5 recites entering the identifier of the functional block and the unique identification of the controller into an encoder; encoding a purchase code as the enable code from the identifier of the functional block and the unique identification of the controller; and selling the purchase code.

Since the references do not teach or suggest encoding or decoding an enable code, they clearly do not contemplate or suggest entering an identifier of a functional block and a unique identification of a controller into an encoder, and encoding a purchase code as an enable code from such identifier of such functional block and such unique identification of such controller. Myers et al., which teaches bank software and bank transactions, such as withdrawing and depositing money, clearly does not teach or suggest selling such a purchase code that was encoded as an enable code. Van Meter et al., which discloses peripherals on a local area network, adds nothing to Myers et al. in this regard. Hence, it is submitted that Claim 5 further patentably distinguishes over the references.

Claims 6-14 and 16-18 are not separately asserted to be patentable except in combination with Claim 5 from which they directly or indirectly depend.

Like Claims 2, 3 and 5, the Examiner states that Claims 15 and 19 recite limitations regarding "typical purchasing/selling situations". Again, those statements are traversed as applied to the refined recital of Applicants' claims, which do not recite "typical purchasing/selling situations". To the extent that the Examiner takes the position that the recitals of Claims 15 and 19 are well known, then it is respectfully requested that the Examiner cite a reference within the context of Applicants' claims.

Claims 15 and 19 depend directly or indirectly from Claims 1 and 14, include all of the limitations thereof, and patentably distinguish over the references for the same reasons.

Furthermore, Claim 15 recites employing a block number as the identifier of the functional block; employing a unique controller number as the unique identification of the controller; inputting the block number and the unique controller number into the encryption algorithm; outputting a purchase code as the enable code from the encryption algorithm; inputting the purchase code into the decryption algorithm; outputting a decrypted block number and a decrypted controller number from the decryption algorithm; and enabling the functional block of the controller when the decrypted block number is equal to the identifier of the functional block and the decrypted controller number is equal to the unique

identification. The references do not teach or suggest the recited enable code from an encryption algorithm, inputting the recited purchase code into a decryption algorithm, outputting a decrypted block number and a decrypted controller number from such decryption algorithm, and enabling a functional block of a controller when such decrypted block number is equal to an identifier of a functional block and such decrypted controller number is equal to a unique identification. Accordingly, Claim 15 further patentably distinguishes over the references.

Furthermore, Claim 19 recites displaying the unique controller number and the block number; informing a supplier of the unique controller number and the block number; and inputting the unique controller number and the block number into the encryption algorithm at a facility of the supplier. Since the references do not teach or suggest the limitations of Claim 15, they clearly do not teach or suggest these additional limitations, which further distinguish over the references.

For the above reasons, it is submitted that Claims 1-19 are in condition for allowance.

Reconsideration and early allowance are requested.

Respectfully submitted,

Kirk D. Houser
Registration No. 37,357
Attorney for Applicants

(412) 566-6083